オープンソースカンファレンス2008 Tokyo/Spring

TOMOYO Linuxで Linuxの動きを学びませう

TOMOYO Linuxプロジェクト
http://tomoyo.sourceforge.jp/
武田健太郎

けふのおはなし

- TOMOYO Linuxの基本
- TOMOYO Linuxでシステムの挙動を把握する方法
  - readaheadのおはなし
- TOMOYO Linux最新動向
  - 次期バージョンで搭載予定の機能
  - 新しいGUI管理ツール

はぢめまして、TOMOYO Linux

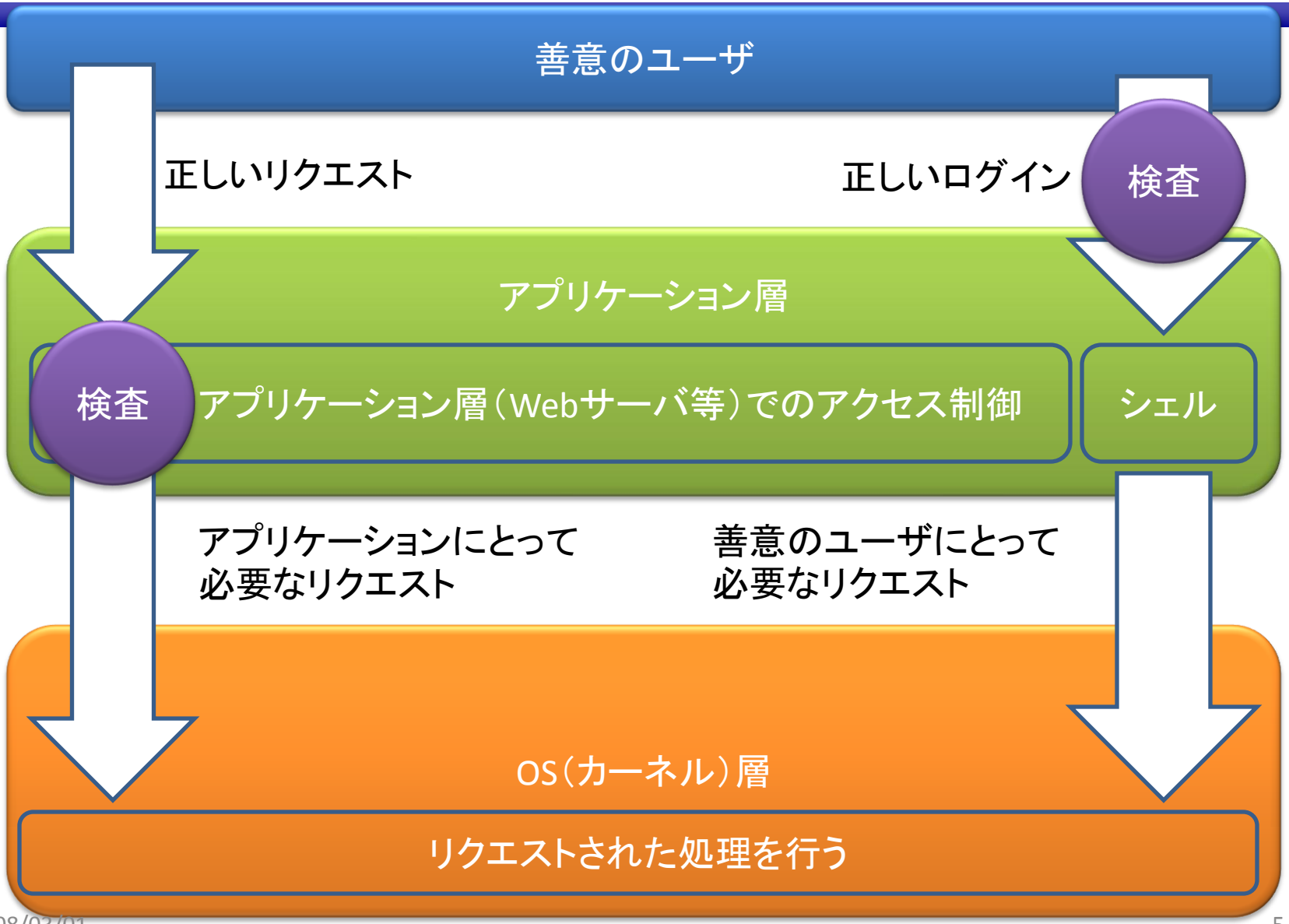
- TOMOYO LinuxはLinux向けのセキュリティ強化技術です
- カーネルレベルで「してよいこと」「わるいこと」を区別します
- 「簡単に使えて安全を保つ」工夫をしています

- ほかのLinuxのセキュリティ強化技術
  - SELinux, AppArmor, LIDS, Smack…

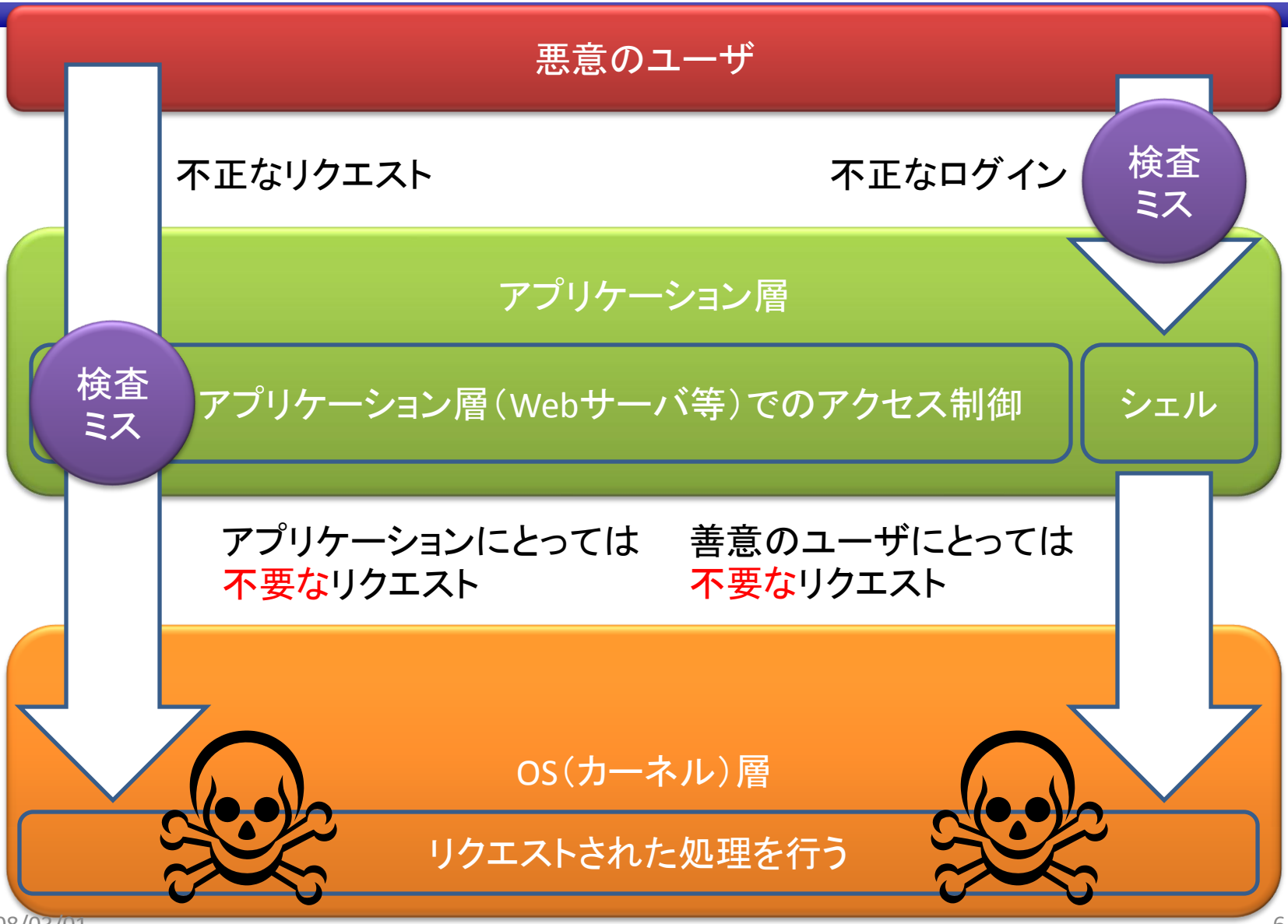
- ひとくちにセキュリティ強化っていっても、どういう風なセキュリティ強化なの？

  ➔カーネルレベルでのアクセスの可否のチェックを追加します

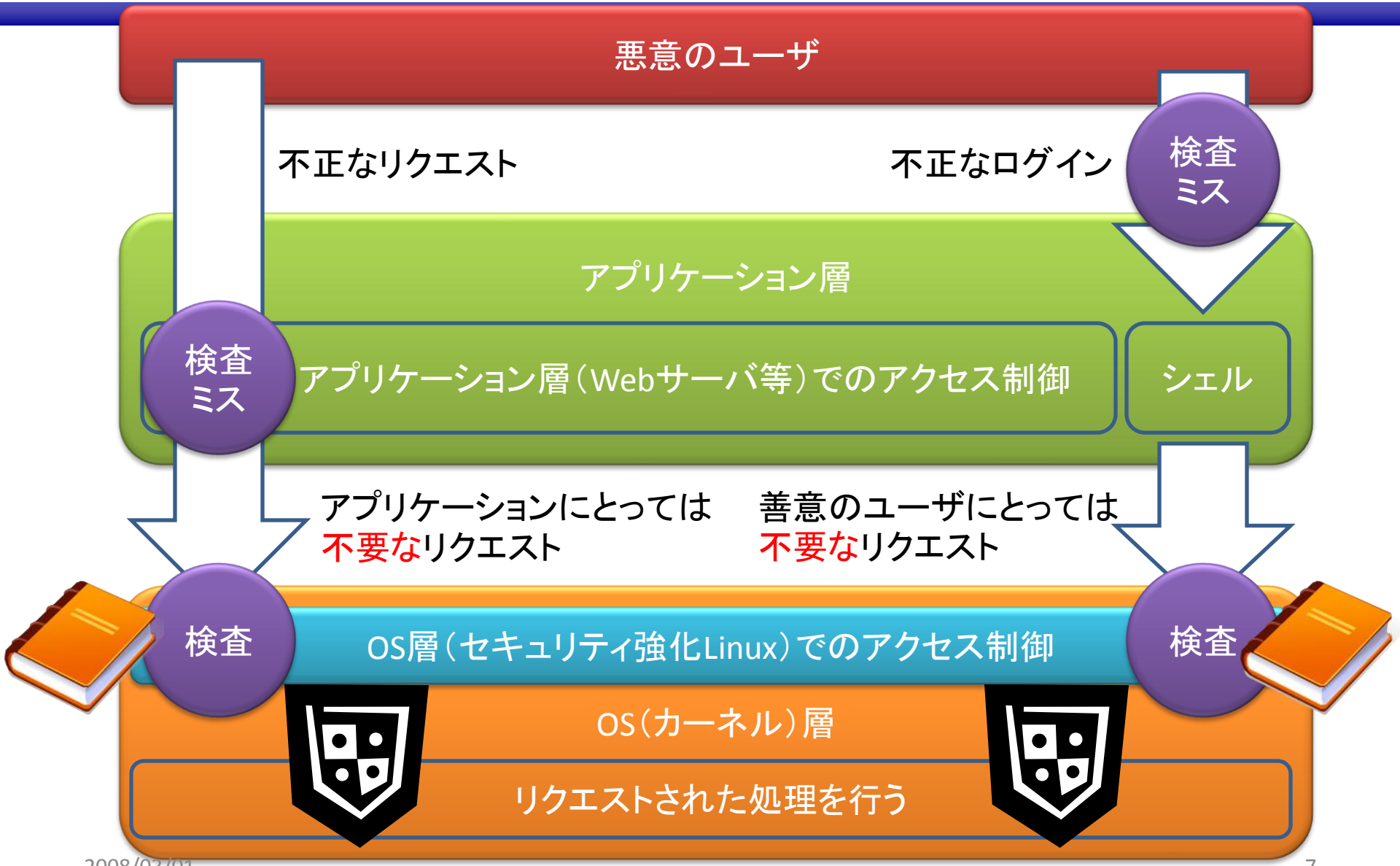
ふつうのLinuxをふつうに使う



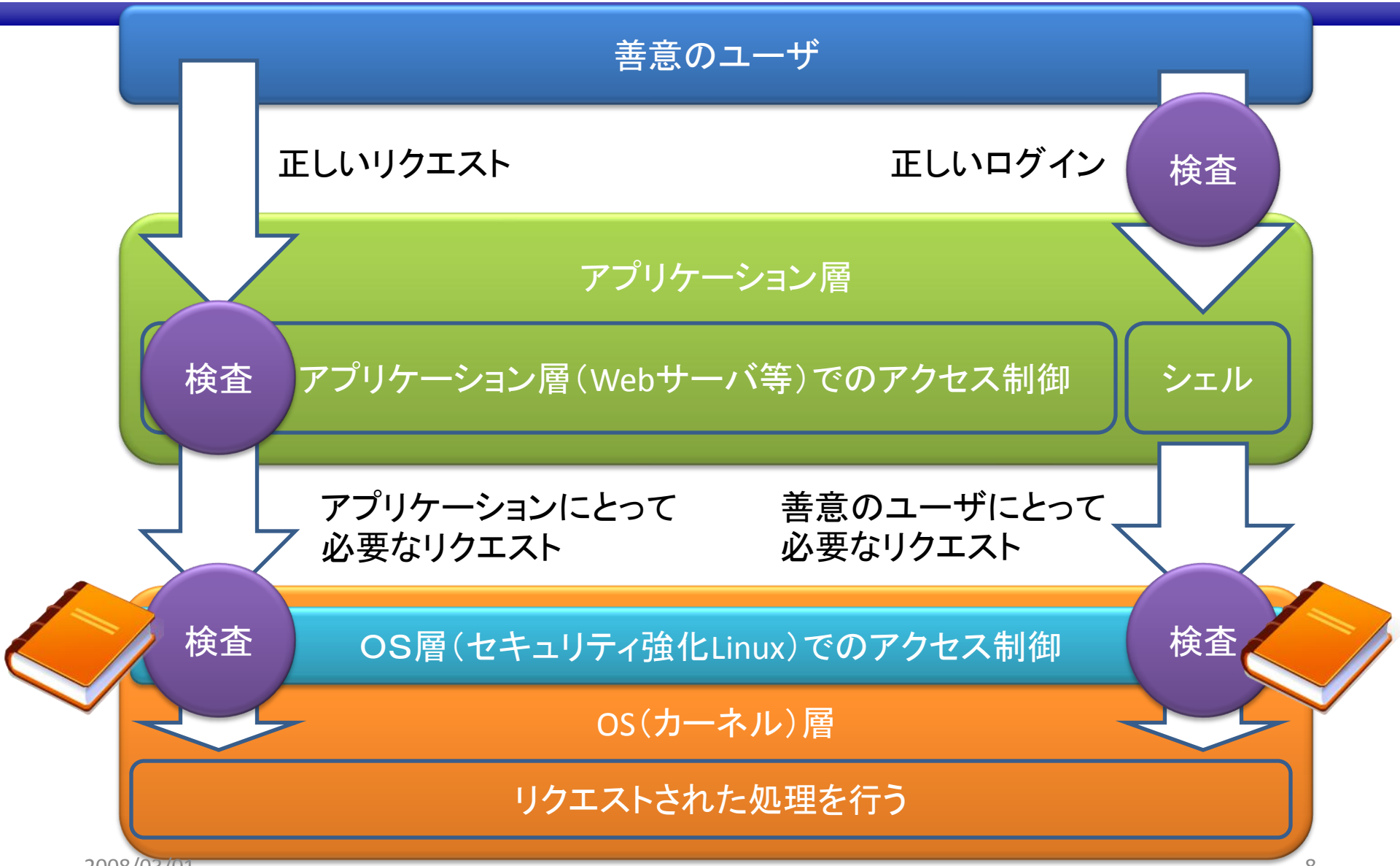
ふつうのLinuxをふつうぢゃなく使う



セキュリティ強化Linuxをふつうぢゃなく使う



セキュリティ強化Linuxをふつうに使う



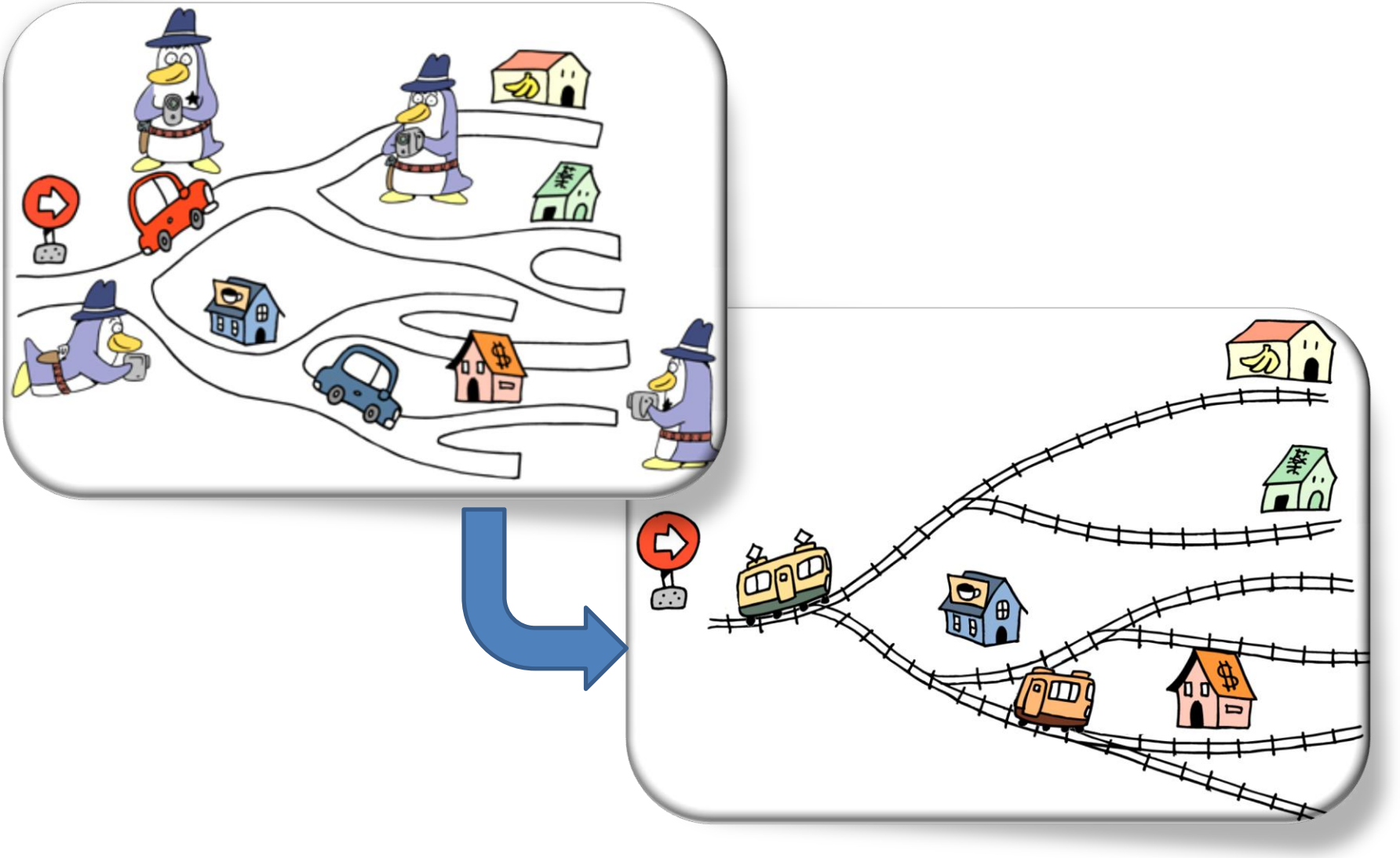
セキュリティ強化OSの設定

- ポリシー
  - セキュリティ強化OSの設定のこと
  - カーネルレベルで「やってよいこと」をすべて記述する必要がある
    - たとえば、「このファイルを読み込んでよい」
    - たとえば、「このIPアドレス・ポート番号でbindしてよい」
  - ポリシーに書いていないことはできない

TOMOYO Linuxの特徴

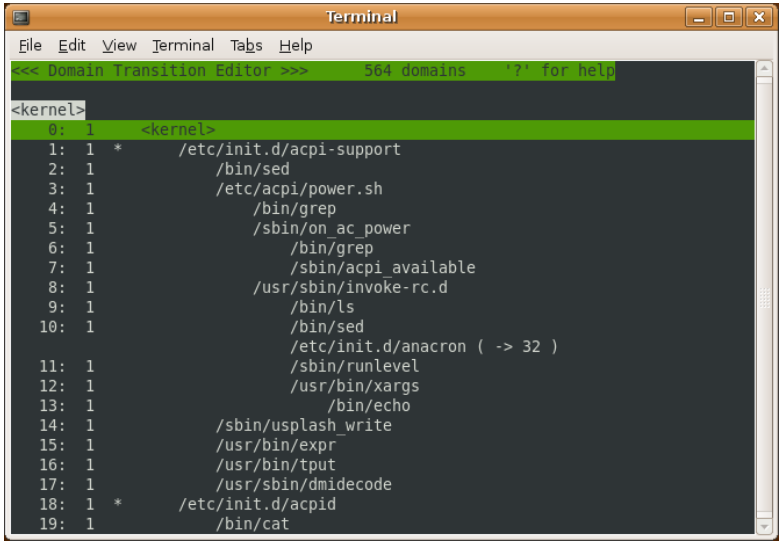
- ポリシーの可読性に優れ、自動学習機能を搭載している
- 自動学習機能の使い方：
  - TOMOYO Linuxを学習モードに設定
    - アプリケーションを動作させる
    - TOMOYO Linuxが動作を学習して自動的にポリシーを作成する
  - TOMOYO Linuxを強制モードに設定
    - 学習させた動作しかおこなえなくなる

自動学習？



自動学習

- 動作を学習するということは、
  - プロセス（主体）の資源（客体）へのアクセスを
  - 監視し
  - 記録する



- 一種のアクセス解析機能
- アクセス解析の結果＝ポリシー

- 具体的にどんな風にアクセス解析に使えるの？
  - ➔TOMOYO Linuxを使ったreadaheadの設定ファイルの作り方を紹介します

readahead

- ファイルを先読みしてメモリキャッシュに乗せて高速化を図る仕組み
- /etc/readahead/bootに列挙されたファイルがシステム起動の初期フェーズにメモリに乗る

- システムが起動するまで読み込まれるファイルを記載する
- この設定ファイルをTOMOYO Linuxを使って作ってみませう

/etc/readahead/bootの作成

- ライブラリファイルなどの読み込みを無条件に許可するallow_readエントリをポリシーから削除
- TOMOYO Linuxを学習モードに設定してシステムを起動
- 以下のプロセスの学習結果を削除
  - /sbin/readahead-list
  - /usr/sbin/gdm
- ポリシーからシステム起動時に読み込んだファイルを抽出！

```
grep '^[1457] ' /proc/ccs/domain_policy | ¥
  cut -c3- | ¥
  sort | uniq | ¥
  egrep '^/bin/|^/etc/|^/lib/|^/sbin/|^/usr/|^/var/' ¥
    > /etc/readahead/boot
```

これ以外にも…

- シェルの設定ファイルって何が読まれるんだっけ？
  - .profile .bash_profile .bash_login .bashrc …
  - …どれがどれだか覚えきれませんorz
- make install時にどんなファイルが配置されるのか知りたいなぁ

- どちらの場合も、TOMOYO Linuxでbashやmakeの動作を学習させれば一発です
  - 実際にTOMOYO GUIの開発や、無線LANドライバをtarballに固めたりする時に大活躍

- で、最近どうなのよ？
  - 開発中のTOMOYO Linux次期バージョンは…
  - 開発中のTOMOYO GUI次期バージョンは…

TOMOYO Linux次期バージョン

- プログラム実行時の引数や環境変数の制限
- プロセスが受け取れる環境変数の制限
- ptraceの制限

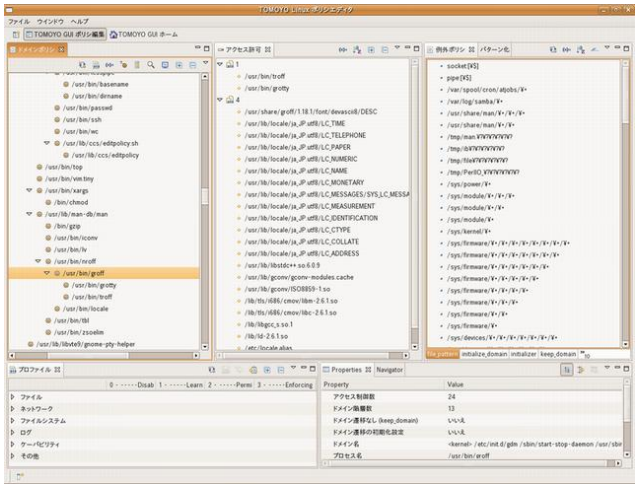
- ポリシー違反時にできることの追加
  - ペナルティとして一定時間眠らせる
  - そもそも別のプロセスに置き換えてしまう

- 1つのプロセス内の「状態」の概念の導入
  - カーネルだけで実現するChangeHat

TOMOYO GUI次期バージョン

- TOMOYO Linuxの管理を行えるGUIツール
  - SSHでTOMOYO Linuxが導入されたマシンに接続
  - WindowsやLinuxのGUIからTOMOYO Linuxを管理

- TOMOYO GUI次期バージョンの目玉
  - TOMOYO Linux 1.5.x, 2.1.xに対応
  - Eclipse RCP化
    - 実行にEclipseが不要に



- もっと自分でためしてみたい！

  ➔TOMOYO Linuxの世界へようこそ！

  各種ドキュメントや資料を整理した記事が
  Software Designの4月号に掲載予定です
  「TOMOYO Linuxの歩き方」

  まずはLiveCDでぐりぐり触ってみてください

TOMOYO Linux Live!

- LiveCD：
  - CDからOSが起動するように作られたシロモノ
- TOMOYO Linux Live!
  - Ubuntu 7.10にTOMOYO Linux1.5.3を導入済
  - いきなり学習モードで起動する
  - システム全体のポリシー（＝アクセス解析結果）がブラウズ可能
  - Linuxの学習に最適！